PATENT COOPERATION TREATY

From	the	INT	ERN	IAT	IONA	L BI	UREAU
------	-----	-----	-----	-----	------	------	-------

To: **PCT Assistant Commissioner for Patents NOTIFICATION OF ELECTION** United States Patent and Trademark (PCT Rule 61.2) Office **Box PCT** Washington, D.C.20231 **ETATS-UNIS D'AMERIQUE** Date of mailing (day/month/year) in its capacity as elected Office 10 October 2000 (10.10.00) Applicant's or agent's file reference International application No. T99004 PCT PCT/DE00/00752 Priority date (day/month/year) International filing date (day/month/year) 12 March 1999 (12.03.99) 13 March 2000 (13.03.00) **Applicant** BRUNE, Peter et al 1. The designated Office is hereby notified of its election made: X in the demand filed with the International Preliminary Examining Authority on: 01 September 2000 (01.09.00) in a notice effecting later election filed with the International Bureau on: 2. The election was not made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland

Authorized officer

Henrik Nyberg

Telephone No.: (41-22) 338.83.38

Facsimile No.: (41-22) 740.14.35

PATENT COOPERATION TREATY From the INTERNATIONAL BUREAU **PCT NOTIFICATION OF THE RECORDING** OF A CHANGE RIEBLING, Peter Postfach 3160 (PCT Rule 92bis.1 and D-88113 Lindau (Bodensee) Administrative Instructions, Section 422) **ALLEMAGNE** Date of mailing (day/month/year) 01 octobre 2001 (01.10.01) Applicant's or agent's file reference IMPORTANT NOTIFICATION T99004 PCT International filing date (day/month/year) International application No. PCT/DE00/00752 13 mars 2000 (13.03.00) 1. The following indications appeared on record concerning: X the agent the applicant the common representative the inventor State of Nationality State of Residence Name and Address **DETEMOBIL** Deutsche Telekom MobilNet GmbH Telephone No. Patentabteilung Landgrabenweg 151 53227 Bonn Facsimile No. Germany Teleprinter No. 2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning: the residence the address the nationality the person the name State of Residence State of Nationality Name and Address RIEBLING, Peter Postfach 3160 Telephone No. D-88113 Lindau (Bodensee) 49-8382-78025/9692-0 Germany Facsimile No. 49-8382-7 80 27

X the International Preliminary Examining Authority	X other: DETEMOBIL-former correspondence add
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Dorothée MÜLHAUSEN
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

Please note the newly-named agent in box 2. All further correspondence should be sent to

Teleprinter No.

the designated Offices concerned

the elected Offices concerned

3. Further observations, if necessary:

the receiving Office

4. A copy of this notification has been sent to:

the International Searching Authority

this address.

09/936420 214

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM **GEBIET DES PATENTWESENS**

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

PCT

REC'D 10 AUG 2001

(Artikel 36 und Regel 70 PCT)

		(Allikei 30 und	negel 70 FC	1)
Aktenzeichen de	s Anmelders oder Anwalts		siehe Mitteil	ung über die Übersendung des internationalen
T99004 PCT		WEITERES VORG	EHEN vorläufigen	Prüfungsberichts (Formblatt PCT/IPEA/416)
Internationales A	ktenzeichen	Internationales Anmelde	edatum <i>(Tag/Monat/Jahr)</i>	Prioritätsdatum (Tag/Monat/Tag)
PCT/DE00/00	752	13/03/2000		12/03/1999
Internationale Pa H04Q7/38	tentklassifikation (IPK) oder i	nationale Klassifikation un	d IPK	
Anmelder				
DETEMOBIL	et al.			
Dieser inte Behörde e	rnationale vorläufige Prüt rstellt und wird dem Anme	fungsbericht wurde vor elder gemäß Artikel 36	der mit der internatio übermittelt.	nalen vorläufigen Prüfung beauftragten
2. Dieser BE	RICHT umfaßt insgesamt	4 Blätter einschließlic	h dieses Deckblatts.	
und/od Behörd	der Zeichnungen, die geä	ndert wurden und dies chtigungen (siehe Rege	em Bericht zugrunde li	ter mit Beschreibungen, Ansprüchen legen, und/oder Blätter mit vor dieser 607 der Verwaltungsrichtlinien zum PCT)
3. Dieser Ber	icht enthält Angaben zu fo	olgenden Punkten:		
ı 🛭	Grundlage des Berichts			
III 🗆	Keine Erstellung eines (Gutachtens über Neuh	eit, erfinderische Tätig	keit und gewerbliche Anwendbarkeit
IV 🗆	Mangelnde Einheitlichke			
v 🛭	Begründete Feststellung gewerblichen Anwendba	g nach Artikel 35(2) hin arkeit; Unterlagen und	sichtlich der Neuheit, d Erklärungen zur Stütz	der erfinderischen Tätigkeit und der ung dieser Feststellung
vı 🗆	Bestimmte angeführte U	-	·	
VII □	Bestimmte Mängel der i	nternationalen Anmeld	ung	
VIII 🗆	Bestimmte Bemerkunge	n zur internationalen A	nmeldung	
Datum der Einreid	chung des Antrags		Datum der Fertigstellun	g dieses Berichts
01/09/2000			08.08.2001	

Bevollmächtigter Bediensteter

von der Straten, G

Tel. Nr. +49 89 2399 8994

Europäisches Patentamt D-80298 München

Prüfung beauftragten Behörde:

Name und Postanschrift der mit der internationalen vorläufigen

Tel. +49 89 2399 - 0 Tx: 523656 epmu d

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE00/00752

I.	Grund	lage o	ies E	3eric	hts
----	-------	--------	-------	-------	-----

1.	Aui ein	fforderung nach Arti	ndteile der internationalen Anm ikel 14 hin vorgelegt wurden, ge hm nicht beigefügt, weil sie kein n:	lten im Rahm	en dieses Berichts als	s "ursprünglich
	1,3	-7	ursprüngliche Fassung			
	2,2	a	eingegangen am	25/05/2001	mit Schreiben vom	22/05/2001
	Pat	entansprüche, Nr.	:			
	1-8		eingegangen am	25/05/2001	mit Schreiben vom	22/05/2001
	Zei	chnungen, Blätter:	:			
	1/1		ursprüngliche Fassung			
2.	die unte Die	internationale Anme er diesem Punkt nic	ne: Alle vorstehend genannten E eldung eingereicht worden ist, z hts anderes angegeben ist. en der Behörde in der Sprache: lelt es sich um	ur Verfügung	oder wurden in dieser	eingereicht, sofern
		die Sprache der Ül Regel 23.1(b)).	bersetzung, die für die Zwecke	der internatio	nalen Recherche eing	ereicht worden ist (nac
		die Veröffentlichun	gssprache der internationalen A	Anmeldung (n	ach Regel 48.3(b)).	
		die Sprache der Ül ist (nach Regel 55.	oersetzung, die für die Zwecke 2 und/oder 55.3).	der internatior	nalen vorläufigen Prüfi	ung eingereicht worder
3.			nternationalen Anmeldung offen e Prüfung auf der Grundlage de			
		in der international	en Anmeldung in schriftlicher Fo	orm enthalten	ist.	
		zusammen mit der	internationalen Anmeldung in o	omputerlesba	arer Form eingereicht v	worden ist.
			achträglich in schriftlicher Form		-	
			achträglich in computerlesbarer	_		
		Die Erklärung, daß	das nachträglich eingereichte s It der internationalen Anmeldun	schriftliche Se	quenzprotokoll nicht ü	
			die in computerlesbarer Form e entsprechen, wurde vorgelegt.	erfassten Info	rmationen dem schriftl	ichen

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE00/00752

4.	Auf	grund der Änderungei	n sind folgen	de U	Interlagen fort	gefaller	า:							
		Beschreibung,	Seiten:											
		Ansprüche,	Nr.:											
		Zeichnungen,	Blatt:											
5.		Dieser Bericht ist ohr angegebenen Gründ eingereichten Fassu	en nach Auf	fassı	ung der Behö	de übe								
		(Auf Ersatzblätter, di beizufügen).	e solche Änd	lerur	ngen enthalter	n, ist un	ter Pu	nkt 1 h	inzuwe	eisen;s	sie sii	ind die	em l	Berich
6.	Etw	aige zusätzliche Bem	erkungen:											
V.		ründete Feststellun verblichen Anwendb											jkeit u	ınd de
1.	Fest	tstellung												
	Neu	heit (N)	_	a: lein:	Ansprüche Ansprüche	1-8								
	Erfir	nderische Tätigkeit (E	•		Ansprüche Ansprüche	1-8								
	Gew	verbliche Anwendbark		a: lein:	Ansprüche Ansprüche	1-8								
2.		erlagen und Erklärung ne Beiblatt	jen											

1. Es wird auf das folgende Dokument verwiesen:

D1 = DE, A, 197 18 103

2. Betreffend Punkt V

a. Der Anspruch 1 betrifft ein Verfahren zur Verteilung von Schlüsseln an Teilnehmer digitaler Mobilfunknetze. Solche Verfahren sind im Prinzip bekannt und zwar insbesondere aus der Druckschrift D1, die als Stand der Technik bezüglich Anspruch 1 angesehen wird.

Dokument D1 offenbart in Übereinstimmung mit dem Oberbegriff des Anspruchs 1 ein Verfahren zur Verteilung von Schlüsseln an beispielsweise Teilnehmer digitaler Mobilfunknetze. Bei dem Verfahren der D1 gibt der Benutzer zum Zwecke seiner Autorisierung zusammen mit seiner Kennung eine Aufforderung zur Auswahl eines Schlüssels ein. Dieser Schlüssel wird dann vom Autorisierungsrechner ausgewählt und an den Benutzer gesendet. Der Benutzer verwendet diesen Schlüssel unmittelbar im weiteren Verlauf des Autorisierungsverfahrens.

Das Verfahren gemäß Anspruch 1 unterscheidet sich von dem aus D1 in bekannten Verfahren durch den kennzeichnenden Teil.

Ein solches Verfahren, bei dem ein Schlüssel einem Teilnehmer zugeordnet und im Endgerät des Teilnehmers abgespeichert wird, ist aus den im Recherchenbericht genannten Dokumenten nicht zu entnehmen und wird durch sie auch nicht nahegelegt. Dieses Verfahren hat den Vorteil, daß der Teilnehmer mehrere Schlüssel speichern kann, die er dann bei Bedarf verwendet.

Der Gegenstand des **Anspruchs 1** ist folglich als neu und erfinderisch anzusehen, Artikel 33 (2) (3) PCT. Der Gegenstand des Anspruchs 1 ist ebenfalls gewerblich anwendbar.

b. Die abhängigen Ansprüche 2 bis 8 beinhalten vorteilhafte Weiterbildungen des Gegenstandes des Anspruchs 1 und erfüllen somit ebenfalls die an sie zu stellenden Anforderungen bezüglich Neuheit, erfinderischer Tätigkeit und gewerblicher Anwendbarkeit.

4:

2

Die DE-A-197 18 103 offenbart ein Verfahren zur Authentisierung in Datenübertragungssystemen, bei dem auf Anfrage eines Teilnehmers ein Schlüssel in Form einer Transaktionsnummer (TAN) von einem im Datenübertragungssystem vorgesehenen Authentisierungsrechner generiert oder aus einer Datei ausgewählt wird. Der Schlüssel wird von dem Authentisierungsrechner an den Teilnehmer übermittelt und kann dort vom Teilnehmer direkt zur Authentifikation gegenüber dem Authentifikationsrechner verwendet werden. Die Verteilung von mehreren Schlüsseln, die vom Teilnehmer je nach Bedarf verwendet werden können, ist aus diesem Dokument nicht zu entnehmen.

Die Aufgabe der Erfindung besteht darin, ein Verfahren anzugeben, durch welches auf gesichertem Wege eine automatisierte Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen erreicht werden kann.

Erfindungsgemäß wird diese Aufgabe durch die kennzeichnenden Merkmale des unabhängigen Patentanspruchs gelöst.

Der Kern der Erfindung besteht darin, dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und ggf. abgespeichert werden, und auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation bzw. das Endgerät des Teilnehmers übertragen wird, wobei der übertragene Schlüssel dem Teilnehmer zugeordnet und im Endgerät und/oder einem Teilnehmeridentitätsmodul (SIM) der Mobilstation zur weitern Verwendung abgespeichert wird.

Das beschriebene Verfahren ist insbesondere geeignet, um auf gesichertem Wege in einem GSM- oder UMTS-Netz automatisiert Schlüssel an mobile Endgeräte zu verteilen und auf der (U)SIM des Teilnehmers zu speichern. Mit diesen Schlüsseln

2 a

kann sich der Nutzer eines Endgeräts gegenüber einem Mehrwertdiensteknoten authentisieren. Mit der (U)SIM steht ein zugriffsgeschütztes Medium zur Verfügung, um Paßwörter bzw. Schlüssel aus einem Mobilfunknetz abzufragen, zu speichern und bei Bedarf zur Authentisierung zu nutzen.

Durch die elektronische und sichere Verteilung und die damit einhergehende Automatisierung besteht zum einen eine deutliche Aufwandsreduktion und Zeitgewinn gegenüber herkömmlichen Schlüsselverteilungsverfahren, die meist auf bestätigtem Schriftverkehr beruhen. Zum anderen führt der automatisierte Ablauf und damit der Ausschluß menschlicher Aktivitäten bei der Schlüsselgenerierung und Verteilung zu einer Erhöhung der Sicherheit.

Die einfache Verteilung erlaubt darüber hinaus eine häufigere Verteilung von Schlüsseln mit niedrigem Aufwand. Dies ermöglicht die Nutzung auch einfacher Authentisierungsverfahren beim Zugang zu Mehrwertdiensteknoten eines Telekommunikationsnetzes, bei denen z.B. ein bestimmter Schlüssel nur ein einziges Mal verwendet wird.

Printed:01-08-2001

8

Patentansprüche

- 1. Verfahren zur Verteilung von Schlüsseln an Teilnehmer digitaler Mobilfunknetze (7), wobei die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung (9) generiert und gegebenenfalls gespeichert werden und auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung (9) angefordert und über das Mobilfunknetz (7) an eine Mobilstation (3) oder ein Endgerät (4) des Teilnehmers übertragen wird, dadurch gekennzeichnet, dass der übertragene Schlüssel dem Teilnehmer zugeordnet und im Endgerät (4) und/oder einem Teilnehmeridentitätsmodul SIM (5) der Mobilstation (3) abgespeichert wird.
- 2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass auf dem Teilnehmeridentitätsmodul SIM (5) der Mobilstation (3) eine SAT-Applikation eingerichtet ist, die eine zusätzliche Ende-Zu-Ende-Verschlüsselung des zwischen Mobilstation (3) und Sicherheitseinrichtung (9) übertragenen Schlüssels vornimmt.
- Verfahren nach Anspruch 2, dadurch gekennzeichnet,
 dass sich der Teilnehmer zur Nutzung der SAT-Applikation gegenüber dem Teilnehmeridentitätsmodul SIM (5) durch Eingabe einer PIN identifizieren muss.
- 4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der übertragene Schlüssel auf einem geschützten Speicherbereich des Teilnehmeridentitätsmoduls SIM (5) abgespeichert wird.
- Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Übertragung des Schlüssels über einen Verkehrskanal des Mobilfunknetzes (7) erfolgt.

9

- Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Übertragung des Schlüssels über einen Signalisierungskanal des Mobilfunknetzes (7) in Form einer Kurznachricht SM erfolgt.
- Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass bei Anforderung des Schlüssel die Berechtigung des Teilnehmers durch Auswertung einer Mobilteilnehmer-Rufnummer MSISDN des Teilnehmers geprüft wird.
- 8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (9) den an den Teilnehmer übermittelten Schlüssel an einen oder mehrere Mehrwertdiensteknoten (11) sendet.

<u>-</u>

If, furthermore, the added value service node is accessed via networks that are not secure, such as the Internet, there is a risk of the user name and password being monitored without authorization, and being misused.

The object of the invention is to specify a method using which keys can be distributed automatically to communications network subscribers using secure means.

According to the invention, this object is achieved by the characterizing features of the independent patent claim.

The essence of the invention is that the keys are generated, and may be stored if required, in a security device provided at the mobile radio network end, and in that on request by a subscriber, a key is requested from the security device, is allocated to the subscriber, and is transmitted via the mobile radio network to the subscriber's mobile station.

The described method is particularly suitable for distributing keys automatically to mobile terminals by secure means in a GSM or UMTS network, and for storing them on the subscriber's (U)SIM. A terminal user can use these keys to authenticate himself to an added value service node. The (U)SIM provides a protected-access medium in order to check passwords or keys, to store them and, when required, to use them for authentication, from a mobile radio network.

Patent Claims

- A method for distributing keys to subscribers in communications networks, in particular digital mobile radio networks, characterized
- in that the keys are generated, and may be stored if required, in a security device provided at the mobile radio network end, and in that on request by a subscriber, at least one key is requested from the security device, is allocated to the subscriber, and is transmitted via the mobile radio network to the subscriber's mobile station/terminal.
- 2. The method as claimed in claim 1, characterized in that an SAT application is set up on the mobile station's SIM, and carries out additional end-to-end encryption of the information transmitted between the mobile station and the security device.
- 3. The method as claimed in claim 1 or 2, characterized in that, in order to use the SAT application, the subscriber must identify himself to the U(SIM) by entering a PIN.
- 4. The method as claimed in one of claims 1 to 3, characterized
- in that the transmitted key is stored in the terminal and/or in the mobile station's subscriber identity module U(SIM).
- 5. The method as claimed in one of claims 1 to 4, characterized
- in that the transmitted key is stored in a protected memory area in the U(SIM).

- 6. The method as claimed in one of claims 1 to 5, characterized
- in that the key is transmitted via a traffic channel in the mobile radio network.
- 7. The method as claimed in one of claims 1 to 5, characterized
- in that the key is transmitted in the form of a short message (SM) via a signaling channel in the mobile radio network.
- 8. The method as claimed in one of claims 1 to 7, characterized
- in that, when the key is requested, the subscriber's authorization is checked by evaluating the mobile subscriber telephone number MSISDN.
- 9. The method as claimed in one of claims 1 to 8, characterized
- in that the security device sends the key which is transmitted to the subscriber to one or more added value service nodes.

PCT/DE00/00752

WO 00/56101

- 1. FIGURE
- 2. Added value service node

09/936420

VERTRAGÜBER DIE INTERNATIONALE ZUGAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts T99004 PCT	WEITERES VORGEHEN		lie Übermittlung des internationalen Formblatt PCT/ISA/220) sowie, soweit nder Punkt 5
Internationales Aktenzeichen	Internationales Anmeld		(Frühestes) Prioritätsdatum (Tag/Monat/Jahr)
PCT/DC 00/00752	(Tag/Monat/Jahr) 13/03/20	200	12/03/1999
PCT/DE 00/00752	13/03/20	J00	12/03/1777
Anmelder			
DETEMOBIL et al.			
Dieser internationale Recherchenbericht wurd Artikel 18 übermittelt. Eine Kopie wird dem In	de von der Internationaler ternationalen Büro überm	n Recherchenbehörde e ittelt.	rstellt und wird dem Anmelder gemäß
Dieser internationale Recherchenbericht umf Narüber hinaus liegt ihm jer	aßt insgesamt <u>2</u> weils eine Kopie der in die	Blätter. esem Bericht genannten	u Unterlagen zum Stand der Technik bei.
Grundlage des Berichts	-		
A. Hinsichtlich der Sprache ist die inte durchgeführt worden, in der sie eine	ernationale Recherche au gereicht wurde, sofern un	f der Grundlage der inte ter diesem Punkt nichts	rnationalen Anmeldung in der Sprache anderes angegeben ist.
Die internationale Recherch Anmeldung (Regel 23.1 b))	ne ist auf der Grundlage e durchgeführt worden.	riner bei der Behörde ei	ngereichten Übersetzung der internationalen
Recherche auf der Grundlage des	Sequenzprotokolls durchç	jeführt worden, das	Aminosäuresequenz ist die internationale
in der internationalen Anme	•		
zusammen mit der internati			ngereicht worden ist.
bei der Behörde nachträglic		-	
bei der Behörde nachträglic			
internationalen Anmeldung	intragiich eingereichte sch im Anmeldezeitpunkt hin	ausgeht, wurde vorgele	oll nicht über den Offenbarungsgehalt der gt.
Die Erklärung, daß die in α wurde vorgelegt.	omputerlesbarer Form erf	aßten Informationen de	m schriftlichen Sequenzprotokoll entsprechen,
2. Bestimmte Ansprüche ha	ben sich als nicht reche	erchierbar erwiesen (si	iehe Feld I).
3. Mangeinde Einheitlichkei			•
4. Hinsichtlich der Bezeichnung der Erfl			
wird der vom Anmelder ein			
wurde der Wortlaut von der	Behörde wie folgt festge	setzt:	
5. Hinsichtlich der Zusammenfassung			
wird der vom Anmelder ein wurde der Wortlaut nach B	egel 38.2b) in der in Feld e innerhalb eines Monats	III angegebenen Fassu	ng von der Behörde festgesetzt. Der Absendung dieses internationalen
6. Folgende Abbildung der Zelchnungen	ist mit der Zusammenfas	sung zu veröffentlichen:	: Abb. Nr
wie vom Anmelder vorgesc	hlagen		keine der Abb.
weil der Anmelder selbst ke	eine Abbildung vorgeschl	agen hat.	
weil diese Abbildung die Er	findung besser kennzeich	nnet.	

PCT/DE 00/00752

A. KLASSII IPK 7	FIZIERUNG DES ANMELDUNGSGEGENSTANDES H04Q7/38 G07F7/10 H04L29/0	6	
4			
Nach der Int	temationalen Patentklassifikation (IPK) oder nach der nationalen Klas	sifikation und der IPK	
	RCHIERTE GEBIETE		
	ter Mindestprüfstoff (Massifikationssystem und Massifikationssymbo H040 G07F H04L	le)	
IPK 7	HU4Q GU/F HU4L		
Rachambian	te aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, so	weit diese unter die recherchierten Gebiete	fallen
Hecherchier	te aper mate zum windestprüston genorende veronendichungen, 30	well diese differ die recherchierten Gestete	TOTAL COLUMN TO THE COLUMN TO
Während de	r internationalen Recherche konsultierte elektronische Datenbank (N	ame der Datenbank und evtl. verwendete S	Suchbegriffe)
EPO-In			• .
LI O III	Cernar		
CAISWE	SENTLICH ANGESEHENE UNTERLAGEN		
Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe	e der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 197 18 103 A (SCHMITZ KIM)		1,4,6-9
	4. Juni 1998 (1998-06-04)		
	das ganze Dokument 		
Α	"GSM TECHNICAL SPECIFICATION GSM	11.14	2,3
	VERSION 5.7.0"	DD VV VV	
	EUROPEAN TELECOMMUNICATION STANDA 1. April 1998 (1998-04-01), Seit		
	COMPLETE66 XP002089350		
	Seite 12 -Seite 13		
			
		<u>.</u>	
		!	
	l Salada Francisco de Francisco Fran	Y Siehe Anhang Patentfamilie	
	tere Veröffentlichungen sind der Fortsetzung von Feld C zu ehmen		
"A" Veröffe	ntlichung, die den allgemeinen Stand der Technik definiert,	"T" Spätere Veröffentlichung, die nach dem oder dem Prioritätsdatum veröffentlich	t worden ist und mit der
abern	iicht als besonders bedeutsam anzusehen ist Dokument, das jedoch erst am oder nach dem internationalen	Anmeldung nicht kollidiert, sondem nu Erfindung zugrundeliegenden Prinzips Theorie angegeben ist	
Anme		"X" Veröffentlichung von besonderer Beder kann allein aufgrund dieser Veröffentlich	utung; die beanspruchte Erfindung
scheir	nen zu lassen, oder durch die das Veröffentlichungsdatum einer	erfinderischer Tätigkeit beruhend betra	ichtet werden
soll oc ausge	der die aus einem anderen besonderen Grund angegeben ist (wie	"Y" Veröffentlichung von besonderer Bedet kann nicht als auf erfinderischer T\u00e4tigk werden, wenn die Ver\u00f6ffentlichung mit	eit beruhend betrachtet
"O" Veröffe eine E	entlichung, die sich auf eine mündliche Offenbarung, Benutzung, eine Ausstellung oder andere Maßnahmen bezieht	Veröffentlichungen dieser Kategorie in diese Verbindung für einen Fachmann	Verbindung gebracht wird und
"P" Veröffe	-Ni-huma dia usa dam internationalan Anmoldodatum abar nach	*& Veröffentlichung, die Mitglied derselber	•
Datum des	Abschlusses der internationalen Recherche	Absendedatum des internationalen Re	cherchenberichts
1	2. Juli 2000	24/07/2000	
Name und	Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter	
	Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk	·	
	Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Leouffre, M	

1

NERNATIONAL SEARCH REPORT

information on patent family members

nternational Application No
PCT/DE 00/00752

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19718103 A	04-06-1998	AU 6354598 A CN 1207533 A EP 0875871 A JP 10341224 A US 6078908 A	05-11-1998 10-02-1999 04-11-1998 22-12-1998 20-06-2000

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7:

H04Q 7/38, G07F 7/10, H04L 29/06

(11) Internationale Veröffentlichungsnummer:

WO 00/56101

A1

(43) Internationales
Veröffentlichungsdatum:

21. September 2000 (21.09.00)

(21) Internationales Aktenzeichen:

PCT/DE00/00752

(22) Internationales Anmeldedatum:

13. März 2000 (13.03.00)

(30) Prioritätsdaten:

199 11 221.5

12. März 1999 (12.03.99)

US

(71) Anmelder (für alle Bestimmungsstaaten ausser US): DE-TEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH [DE/DE]; Deutsche Telekom MobilNet GmbH, Landgrabenweg 151, D-53227 Bonn (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): BRUNE, Peter [DE/DE]; Noldestrasse 56, D-53340 Meckenheim (DE). SASSE, Andreas [DE/DE]; Zur Mühle 13, D-53773 Hennef (DE). (81) Bestimmungsstaaten: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CZ, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht

Mit internationalem Recherchenbericht. Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

- (54) Title: METHOD OF DISTRIBUTING KEYS TO SUBSCRIBERS OF COMMUNICATIONS NETWORKS
- (54) Bezeichnung: VERFAHREN ZUR VERTEILUNG VON SCHLÜSSELN AN TEILNEHMER VON KOMMUNIKATIONSNETZEN

(57) Abstract

The invention relates to a method of distributing keys to subscribers of communications networks, especially of digital mobile radio networks. Said keys are required, for example, for accessing value-added services. The aim of the invention is to provide a method for distributing said keys to the subscribers safely and above all in an uncomplicated manner. To this end, the keys are generated and optionally saved in a safety device provided at the end of the mobile radio network. Upon request of a subscriber, at least one key is requested from said safety device, is allocated to the subscriber and is transmitted to the mobile station of the subscriber via the mobile radio network.

(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren zur Verteilung von Schlisseln an Teilnehmer von Kommunikationsnetzen, insbesondere digitalen Mobilfunknetzen. Diese Schlüssel werden z.B. für den Zugang zu Mehrwertdiensten benötigt. Hierbei besteht das Problem, die Schlüssel sicher und vor allem unkompliziert an die Teilnehmer zu verteilen. Erfindungsgemäss wird dies dadurch erreicht, dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und gegebenenfalls gespeichert werden, und auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation des Teilnehmers übertragen wird.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

					•		
AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK ·	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
ΑÜ	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldan	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische	TM ·	Turkmenistan
BF	Burkina Faso	GR	Griechenland		Republik Mazedonien	TR	Türkei
BG	Bulgarien	HU	Ungam	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von
CA	Kanada	IT	Italien	MX	Mexiko		Amerika
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan.
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Victnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik	NZ	Neusceland	zw	Zimbabwe
CM	Kamerun		Korea	PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		•
DK	Dānemark	LK	Sri Lanka	, SE	Schweden		
EE	Estland	LR	Liberia	" SG	Singapur		

Verfahren zur Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen

Die Erfindung betrifft ein Verfahren zur Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen, insbesondere digitalen Mobilfunknetzen, nach dem Oberbegriff des unabhängigen Patentanspruchs. Mit diesen Schlüsseln kann sich der Nutzer eines Endgeräts z.B. gegenüber einem Mehrwertdiensteknoten des Kommunikationsnetzes authentisieren.

Heute authentisiert sich ein Teilnehmer von Telekommunikationsdiensten beim Zugang zu Mehrwertdiensteknoten wie z. B. einer Mobilbox, durch Eingabe eines Paßworts und Nutzernamens. In GSM-Mobilfunknetzen wird dabei meist durch die Signalisierung die Mobilteilnehmer-Rufnummer (MSISDN) als Nutzemame übertragen, womit eine explizite Angabe durch den Nutzer entfällt.

Die Vergabe und Nutzung des Paßworts (hier gleichbedeutend mit Schlüssel) ist ein kritischer Vorgang, da durch unerwünschte Offenlegung oder bewußtes Ausspähen dem Nutzer erheblicher Schaden durch Mißbrauch zugefügt werden kann. Neue Paßwörter werden daher häufig per Einschreibebrief versandt, was organisatorisch und technisch einen erheblichen Aufwand bedeutet und zugleich einen Zeitverzug, bis ein Paßwort beim Nutzer eintrifft.

Geschieht darüber hinaus der Zugang zum Mehrwertdiensteknoten über unsichere Netze wie z. B. das Internet, besteht die Gefahr, daß Nutzername und Paßwort unberechtigterweise abgehört und mißbraucht werden.

Die Aufgabe der Erfindung besteht darin, ein Verfahren anzugeben, durch welches auf gesichertem Wege eine automatisierte Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen erreicht werden kann.

Erfindungsgemäss wird diese Aufgabe durch die kennzeichnenden Merkmale des unabhängigen Patentanspruchs gelöst.

Der Kem der Erfindung besteht darin, dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und ggf. abgespeichert werden, und auf Anfrage eines Teilnehmers ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation des Teilnehmers übertragen wird.

Das beschriebene Verfahren ist insbesondere geeignet, um auf gesichertem Wege in einem GSM- oder UMTS-Netz automatisiert Schlüssel an mobile Endgeräte zu verteilen und auf der (U)SIM des Teilnehmers zu speichem. Mit diesen Schlüsseln kann sich der Nutzer eines Endgeräts gegenüber einem Mehrwertdiensteknoten authentisieren. Mit der (U)SIM steht ein zugriffsgeschütztes Medium zur Verfügung, um Paßwörter bzw. Schlüssel aus einem Mobilfunknetz abzufragen, zu speichern und bei Bedarf zur Authentisierung zu nutzen.

Durch die elektronische und sichere Verteilung und die damit einhergehende Automatisierung besteht zum einen eine deutliche Aufwandsreduktion und Zeitgewinn gegenüber herkömmlichen Schlüsselverteilungsverfahren, die meist auf bestätigtem Schriftverkehr beruhen. Zum anderen führt der automatisierte Ablauf und damit der Ausschluß menschlicher Aktivitäten bei der Schlüsselgenerierung und Verteilung zu einer Erhöhung der Sicherheit.

Die einfache Verteilung erlaubt darüber hinaus eine häufigere Verteilung von Schlüsseln mit niedrigem Aufwand. Dies ermöglicht die Nutzung auch einfacher Authentisierungsverfahren beim Zugang zu Mehrwertdiensteknoten eines Telekommunikationsnetzes, bei denen z.B. ein bestimmter Schlüssel nur ein einziges Mal verwendet wird.

Der berechtigte Nutzer der (U)SIM kann die Möglichkeit nutzen, den Schlüssel in andere Endgeräte zu transferieren bzw. mit dem mobilen oder anderen Endgeräten über Internet, PSTN oder ISDN auf die Mehrwertdiensteknoten zuzugreifen. Das Authentikationsverfahren zwischen Endgerät und Mehrwertdiensteknoten sowie der Transfer eines Schlüssels vom mobilen Endgerät auf ein anderes kann mit bestehenden Algorithmen gelöst werden und ist nicht Gegenstand der Erfindung.

In einer ersten Ausführungsvariante der Erfindung ist vorgesehen, dass der Nutzer einen neuen Schlüssel bei Bedarf durch eine Kurznachricht (SMS) abruft. Dazu sendet er eine Kurznachricht mit bestimmten Inhalt an eine durch den Netzbetreiber vorgegebene Zieladresse, die einer Sicherheitseinrichtung zugeordnet ist. Als Antwort erhält er von dieser Adresse ein Paßwort im Klartext zurück. Mit diesem Paßwort kann sich der Nutzer nun gegenüber einem Mehrwertdiensteknoten authentisieren.

In einer zweiten Ausführungsvariante der Erfindung, die ein höheres Sicherheitsniveau aufweist, ist vorgesehen, dass durch die Verwendung eines Programms auf der (U)SIM (Kartenapplikation), welches als Client mit dem Mobilfunknetz kommuniziert, alle Kommunikationsvorgänge zwischen Mobilstation und Sicherheitseinrichtung mit einem Ende-zu-Ende Verschlüsselungsverfahren verschlüsselt werden. In vorteilhafter Weise kann das Programm dem Nutzer eine menügeführte Oberfläche auf dem mobilen Endgerät bieten, mit der Schlüssel abgerufen und verwaltet werden können.

Zur Anforderung eines Schlüssels wählt der Nutzer z.B. einen entsprechenden Menüpunkt auf seinem Endgerät. Das Mobilfunknetz antwortet mit einer verschlüsselten Nachricht, die direkt an die Kartenapplikation gerichtet ist. Die Kartenapplikation speichert den Schlüssel in einem geschützten Speicherbereich der (U)SIM ab.

Zur Authentisierung gegenüber einem Mehrwertdiensteknoten wählt der Nutzer nach Eingabe einer PIN z.B. einen entsprechenden Menüpunkt an. Je nach Authentisierungsalgorithmus ist vorgesehen, dass

- der Schlüssel entweder im Klartext angezeigt und kann vom Nutzer weiterverwendet werden kann;
- der Schlüssel direkt zum Mehrwertdiensteknoten übertragen wird;
- der Schlüssel zu einem anderen Endgerät transferiert und dort weiterverwendet werden kann.

Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

Im folgenden wird die Erfindung anhand eines Beispiels unter Bezugnahme auf eine Zeichnungsfigur näher beschrieben. Aus dem Beispiel, der Zeichnung und ihrer Beschreibung gehen weitere Merkmale und Vorteile der Erfindung hervor

Figur 1 zeigt eine Darstellung der beteiligten Systeme zur Durchführung des Verfahrens.

Die Mobilstation 3, welche ein Endgerät 4 umfasst, beherbergt in bekannter Weise die (U)SIM 5, auf der die Schlüssel zur Nutzerauthentikation gespeichert werden. Die Sicherheitseinrichtung umfasst einen Sicherheits-Server 9, der die Schlüssel nach einem vom Betreiber gewählten Algorithmus erzeugt, in einer Datenbank 10 speichert und die Schlüssel auf Anforderung 1 eines Teilnehmers an die (U)SIM 5 und die vom Teilnehmer nutzbaren Mehrwertdiensteknoten 11 verteilt.

Das Short Message Service Center 8 des Mobilfunknetzes 7 übermittelt die Schlüssel in Form von Kurznachrichten (SM) 2 zwischen Sicherheits-Server 9 und Mobilstation 3. Dies ist hier nur beispielhaft angegeben. Als Übermittlungseinrichtungen können z. B. auch GPRS-Knoten verwendet werden.

Gemäss einer ersten beim erfindungsgemässen Verfahren angewandten Sicherheitsstufe fordert der Teilnehmer einen Schlüssel über seine Mobilstation 3 durch eine Kurznachricht 1 an.

Der Sicherheits-Server 9 wertet die Anforderung aus, indem die Absendeadresse (MSISDN) des Teilnehmers auf Berechtigung geprüft wird, und sendet den oder die Schlüssel in einer Kurznachricht 2 an die Mobilstation 3, wo sie auf der (U)SIM 5 gespeichert wird. Darüber hinaus sendet der Sicherheits-Server 9 den Schlüssel an einen oder mehrere Mehrwertdiensteknoten 11. Die Schlüsselverteilung ist damit beendet. Der Nutzer kann sich nun je nach gewähltem Endgerät 4 und Zugangsweg (Mobilfunk, ISDN, Internet, etc.) gegenüber dem Mehrwertdiensteknoten 11 authentisieren.

Bei dieser niedrigen ersten Sicherheitsstufe basiert die Sicherheit der Schlüsselverteilung auf der Abhörsicherheit des GSM-/UMTS-Netzes und der Nutzeridentifikation per MSISDN. Einmal auf der (U)SIM gespeichert sind die Schlüssel über die Standard-PIN geschützt.

Bei der zweiten, erhöhten Sicherheitsstufe kann das SIM Application Toolkit (SAT) nach GSM 11.14 eingesetzt werden. Dazu wird eine SAT-Applikation auf die (U)SIM 5 eingebracht, die in dieser Client-Server-Konfiguration mit dem Sicherheits-Server 9 über das GSM- oder UMTS-Netz 7 kommuniziert.

Der Nutzer fordert Schlüssel über sein Endgerät 4 menüunterstützt über die SAT-Applikation an. Dazu muß er sich gegenüber der (U)SIM 5 mit einer zweiten PIN identifizieren, die er z.B. über die Tastatur des Endgeräts 4 eingibt. Danach versendet die SAT-Applikation eine verschlüsselte Anforderung 1 an den Sicherheits-Server 9, der die Anforderung verarbeitet. Der Sicherheits-Server 9 prüft die verschlüsselte Anforderung auf Echtheit anhand der Verschlüsselung sowie der Absendeadresse (MSISDN).

Bei positiv ausgefallener Prüfung erzeugt der Sicherheits-Server 9 den oder die Schlüssel für den Nutzer und sendet sie an die SAT-Applikation der (U)SIM 5 zurück. Die SAT-Applikation nimmt die Schlüssel entgegen und speichert sie in einem besonders geschützten Bereich der (U)SIM 5 ab. Darüber hinaus sendet der

Sicherheits-Server 9 den Schlüssel an einen oder mehrere Mehrwertdiensteknoten 11.

Der Zugriff auf die Schlüssel ist wiederum menügesteuert nach Eingabe einer PIN über die Kartenapplikation möglich, die einen ungebrauchten Schlüssel auf dem Display des Endgeräts 4 anzeigt oder auf Wunsch in einem ungeschützten SIM-Kartenspeicherbereich ablegt. Von dort kann dieser Schlüssel in einen PC/Laptop mittels Standard-Zugriffssoftware ausgelesen werden, z. B. mittels Chipkartenleser oder Infrarot-Schnittstelle des GSM-/UMTS-Endgeräts.

Alternativ und je nach Sicherheitsanforderung kann der Schlüssel auch vor dem Nutzer verborgen bleiben und vertraulich zwischen (U)SIM 5 und Mehrwertdiensteknoten 11 bzw. von der (U)SIM 5 zum Laptop/PC zwecks späterer Verwendung übertragen werden.

Ein besonderes Kennzeichen der zweiten Sicherheitsstufe ist eine zusätzliche Verschlüsselung der ausgetauschten Kurznachrichten 1, 2 zwischen dem Sicherheits-Server 9 (Server-SW) und der Software auf der (U)SIM 5 (Client-SW). Dadurch ist eine Ende-zu-Ende-Sicherheit zwischen Server-SW und Client-SW gegeben. Der Nutzer hat dabei vorzugsweise keine Kenntnis der dazu notwendigen Schlüssel. Als Verschlüsselungsalgorithmen zwischen Client und Server können Standardverfahren wie z. B. Triple-DES oder RSA zum Einsatz kommen.

Die für die Zusatzverschlüsselung notwendigen Schlüssel werden einmalig bei Personalisierung der (U)SIM eingebracht sowie auf den Sicherheits-Server geladen.

Zeichnungslegende

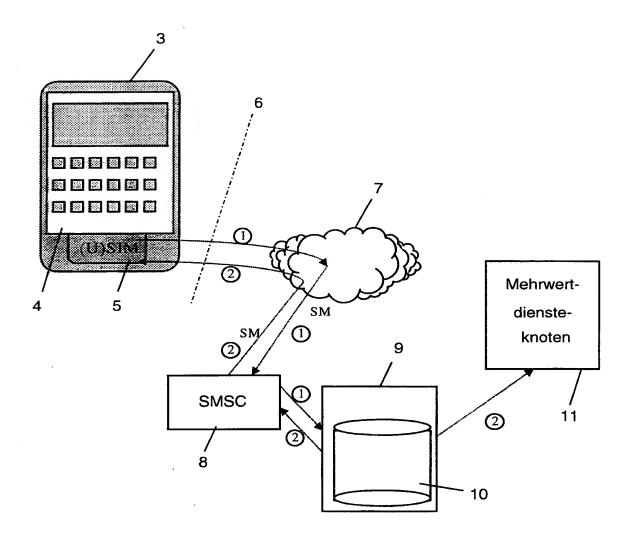
1 Signalfl	uss: Schlüssel	anfordem
------------	----------------	----------

- 2 Signalfluss: Schlüssel laden
- 3 Mobilstation
- 4 Endgerät
- 5 (U)SIM
- 6 Luftschnittstelle
- 7 Mobilfunknetz
- 8 Kurznachrichtendienst-Zentrale
- 9 Sicherheitseinrichtung (Server)
- 10 Datenbank
- 11 Mehrwertdiensteknoten

Patentansprüche

- 1. Verfahren zur Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen, insbesondere digitalen Mobilfunknetzen, dadurch gekennzeichnet, dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und gegebenenfalls gespeichert werden, und dass auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation/ Endgerät des Teilnehmers übertragen wird.
- Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass auf der SIM der Mobilstation eine SAT-Applikation eingerichtet ist, die eine zusätzliche Ende-Zu-Ende-Verschlüsselung der zwischen Mobilstation und Sicherheitseinrichtung übertragenen Informationen vornimmt.
- Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet,
 dass sich der Teilnehmer zur Nutzung der SAT-Applikation gegenüber der
 (U)SIM durch Eingabe einer PIN identifizieren muss.
- Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der übertragene Schlüssel im Endgerät und/oder dem Teilnehmeridentitätsmodul U(SIM) der Mobilstation abgespeichert wird.
- Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass der übertragene Schlüssel auf einem geschützten Speicherbereich der U(SIM) abgespeichert wird.

- Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Übertragung des Schlüssels über einen Verkehrskanal des Mobilfunknetzes erfolgt.
- 7. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass die Übertragung des Schlüssels über einen Signalisierungskanal des Mobilfunknetzes in Form einer Kurznachricht (SM) erfolgt.
- 8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass bei Anforderung des Schlüssel die Berechtigung des Teilnehmers durch Auswertung der Mobilteilnehmer-Rufnummer MSISDN geprüft wird.
- 9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die Sicherheitseinrichtung den an den Teilnehmer übermittelten Schlüssel an einen oder mehrere Mehrwertdiensteknoten sendet.



FIGUR 1

BERICHTIGTE FASSUNG

9/936420

(19) Weltorganisation für geistiges Eigentum Internationales Büro



(43) Internationales Veröffentlichungsdatum 21. September 2000 (21.09.2000)

PCT

(10) Internationale Veröffentlichungsnummer WO 00/56101 A1

(51) Internationale Patentklassifikation⁷: G07F 7/10. H04L 29/06

H04Q 7/38.

(21) Internationales Aktenzeichen: P

PCT/DE00/00752

(22) Internationales Anmeldedatum:

13. März 2000 (13.03.2000)

(25) Einreichungssprache:

Deutsch

(26) Veröffentlichungssprache:

Deutsch

(30) Angaben zur Priorität:

199 11 221.5

12. März 1999 (12.03.1999) DE

- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): DETEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH [DE/DE]: Deutsche Telekom MobilNet GmbH. Landgrabenweg 151, D-53227 Bonn (DE).
- (72) Erfinder; und
- (75) Erfinder/Anmelder (mar für US): BRUNE, Peter [DE/DE]; Noldestrasse 56, D-53340 Meckenheim (DE). SASSE, Andreas [DE/DE]; Zur Mühle 13, D-53773 Hennel (DE).
- (74) Anwalt: RIEBLING, Peter: Postfach 3160, D-88113 Lindau (Bodensee) (DE).

- (81) Bestimmungsstaaten (national): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CZ, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Bestimmungsstaaten (regional): ARIPO-Patent (GH. GM. KE, LS. MW. SD. SL. SZ. TZ, UG, ZW), eurasisches Patent (AM. AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

- mit internationalem Recherchenbericht
- (48) Datum der Veröffentlichung dieser berichtigten Fassung: 30. Mai 2002
- (15) Informationen zur Berichtigung: siehe PCT Gazette Nr. 22/2002 vom 30. Mai 2002. Section II

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

- (54) Title: METHOD OF DISTRIBUTING KEYS TO SUBSCRIBERS OF COMMUNICATIONS NETWORKS
- (54) Bezeichnung: VERFAHREN ZUR VERTEILUNG VON SCHLÜSSELN AN TEILNEHMER VON KOMMUNIKATIONS-NETZEN
- (57) Abstract: The invention relates to a method of distributing keys to subscribers of communications networks, especially of digital mobile radio networks. Said keys are required, for example, for accessing value-added services. The aim of the invention is to provide a method for distributing said keys to the subscribers safely and above all in an uncomplicated manner. To this end, the keys are generated and optionally saved in a safety device provided at the end of the mobile radio network. Upon request of a subscriber, at least one key is requested from said safety device, is allocated to the subscriber and is transmitted to the mobile station of the subscriber via the mobile radio network.
- (57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Verteilung von Schlisseln an Teilnehmer von Kommunikationsnetzen, insbesondere digitalen Mobilfunknetzen. Diese Schlüssel werden z.B. für den Zugang zu Mehrwertdiensten benötigt. Hierbei besteht das Problem, die Schlüssel sicher und vor allem unkompliziert an die Teilnehmer zu verteilen. Erfindungsgemäss wird dies dadurch erreicht, dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und gegebenenfalls gespeichert werden, und auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation des Teilnehmers übertragen wird.



561

2

Die DE-A-197 18 103 offenbart ein Verfahren zur Authentisierung in Datenübertragungssystemen, bei dem aut Anfrage eines Teilnehmers ein Schlüssel in Form einer Transaktionsnummer (TAN) von einem im Datenübertragungssystem vorgesehenen Authentisierungsrechner generiert oder aus einer Datei ausgewählt wird. Der Schlüssel wird von dem Authentisierungsrechner an den Teilnehmer übermittelt und kann dort vom Teilnehmer direkt zur Authentifikation gegenüber dem Authentifikationsrechner verwendet werden. Die Verteilung von mehreren Schlüsseln, die vom Teilnehmer je nach Bedarf verwendet werden können, ist aus diesem Dokument nicht zu entnehmen.

Die Aufgabe der Erfindung besteht darin, ein Verfahren anzugeben, durch welches auf gesichertem Wege eine automatisierte Verteilung von Schlüsseln an Teilnehmer von Kommunikationsnetzen erreicht werden kann.

Erfindungsgemäß wird diese Aufgabe durch die kennzeichnenden Merkmale des unabhängigen Patentanspruchs gelöst.

Der Kern der Erfindung besteht darin, dass die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitseinrichtung generiert und ggf. abgespeichert werden, und auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung angefordert, dem Teilnehmer zugeordnet und über das Mobilfunknetz an die Mobilstation bzw. das Endgerät des Tellnehmers übertragen wird, wobei der übertragene Schlüssel dern Teilnehmer zugeordnet und im Endgerät und/oder einem Teilnehmeridentitätsmodul (SIM) der Mobilstation zur weitern Verwendung abgespeichert wird.

Das beschriebene Verfahren ist insbesondere geelgnet, um auf gesichertem Wege in einem GSM- oder UMTS-Netz automatisiert Schlüssel an mobile Endgeräte zu verteilen und auf der (U)SIM des Teilnehmers zu speichern. Mit diesen Schlüsseln

25-05-200

2 a

kann sich der Nutzer eines Endgeräts gegenüber einem Mehrwertdichsteknoten authentisieren. Mit der (U)SIM steht ein zugriffsgeschütztes Medium zur Verfügung, um Paßwörter bzw. Schlüssel aus einem Mobilfunknetz abzufragen, zu speichern und bei Bedarf zur Authentisierung zu nutzen.

Durch die elektronische und sichere Verteilung und die damit einhergehende Automatisierung besteht zum einen eine deutliche Aufwandsreduktion und Zeitgewinn gegenüber herkömmlichen Schlüsselverteilungsverfahren, die meist auf bestätigtem Schriftverkehr beruhen. Zum anderen führt der automatisierte Ablauf und damit der Ausschluß menschlicher Aktivitäten bei der Schlüsselgenerierung und Verteilung zu einer Erhöhung der Sicherheit.

Die einfache Vertellung erlaubt darüber hinaus eine häufigere Verteilung von Schlüsseln mit niedrigem Aufwand. Dies ermöglicht die Nutzung auch einfacher Authentisierungsverfahren beim Zugang zu Mehrwertdiensteknoten eines Telekommunikationsnetzes, bei denen z.B. ein bestimmter Schlüssel nur ein einziges Mal verwendet wird.

8

Patentansprüche

- 1. Verfahren zur Verteilung von Schlüsseln an Teilnehmer digitaler Mobilfunknetze (7), wohei die Schlüssel in einer auf Mobilfunknetzseite vorgesehenen Sicherheitselnrichtung (9) generiert und gegebenenfalls gespeichert werden und auf Anfrage eines Teilnehmers mindestens ein Schlüssel von der Sicherheitseinrichtung (9) angefordert und über das Mobilfunknetz (7) an eine Mobilstation (3) oder ein Endgerät (4) des Teilnehmers übertragen wird, dadurch gekennzeichnet, dass der übertragene Schlüssel dem Teilnehmer zugeordnet und im Endgerät (4) und/oder einem Teilnehmeridentitätsmodul SIM (5) der Mobilstation (3) abgespeichert wird.
- 2. Verfahren nach Anspruch 1. dadurch gekennzeichnet,
 dass auf dem Teilnehmeridentitätsmodul SIM (5) der Mobilstation (3) eine SATApplikation eingerichtet ist, die eine zusätzliche Ende-Zu-Ende-Verschlüsselung
 des zwischen Mobilstation (3) und Sicherheitseinrichtung (9) übertragenen
 Schlüssels vornimmt.
- Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass sich der Teilnehmer zur Nutzung der SAT-Applikation gegenüber dem Teilnehmeridentitätsmodul SIM (5) durch Eingabe einer PIN identifizieren muss.
- 4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der übertragene Schlüssel auf einem geschützten Speicherbereich des Teilnehmeridentitätsmoduls SIM (5) abgespeichert wird.
- Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Übertragung des Schlüssels über einen Verkehrskanal des Mobilfunknetzes (7) erfolgt.

25-05-200

Printed:01-08-2001

9

- 6. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Übertragung des Schlüssels über einen Signalisierungskanal des Mobilfunknetzes (7) in Form einer Kurznachricht SM erfolgt.
- 7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet.
 dass bei Anforderung des Schlüssel die Berechtigung des Teilnehmers durch
 Auswertung einer Mobilteilnehmer-Rufnummer MSISDN des Teilnehmers geprüft
 wird.
- 8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Sicherheitseinrichtung (9) den an den Teilnehmer übermittelten Schlüssel an einen oder mehrere Mehrwertdiensteknoten (11) sendet.

INTERNATIONALER RECHERCHENBERICHT

PCT/DE 00/00752

A KLASCIPZIERUNG DES AMMELDUNGSGEGENSTANDES 1PK 7 110407/38 G07F7/10 H04L2	9/06
••••	
Nach der Internationalen Patentklassifikration (IPK) oder nach der nationaler	n Klassifikaisını und der ITK
Deshartmener Mindestordistud (Idasoilliationasyotom in Rassilliation	(Wapale)
IN A HOME GOLL HOAT	
Recherchierte aber nicht zum Mindestprüdstoff gehörende Veratientschung	en, soweit disse unter die rechterbierten Geblete tallen
Während der Internationalen Hecherche ku sultierte elektrorische Daterb	onk (Name der Datenbank und evs. verwendete Suchbegnine)
Während der Internationalen Hecherche kur suttlerte diettruste	
EPO-Internal	·
C. ALS WESENTLICH ANGESEHENE UNTERLAGEN	Dotr. Anopruch Nr.
C. ALS WESENTLICH ANGESENTLY STATEMENT OF ST	Angabe der in Betracht kommonden Telle
X DE 197 18 103 A (SCHMITZ KIM) 4. Juni 1998 (1998-06-04)	1,4,6-9
das ganze Dokument "GSM TECHNICAL SPECIFICATION VERSION 5.7.0"	
EURUPEAN TELECOMMUNICATION ST 1. April 1998 (1998-04-01), COMPLETEGO XP002089350 Seite 12 -Seite 13	ANDARD,XX,XX, Seite
Woltern Veröffentlichungen eind der Foresetzung von Heid C zu	X Sieho Anhang Patentiamilia
*Besondere Kalagorien von angegebenen Verülleritschungen : 'A' Verölfenfichung, die den allgemeinen Stand der I echnik gelinten, aber nicht als besonders bedaussam anzuseren itst aber nicht als besonders bedaussam anzuseren itst "E" älteres Dotament, des jedoch enst am oder nach dem international Anmeidedaum veriffendlicht worden ist. 'L' Verölfentlich ang, die geeignat ist, einen Prioritälssangnuch zweifelt scheinen zu lassen, oder durch die der Verölfentlichtung belegt entleten im Rechosohombesicht genammen Verölfentlichtung belegt ausgeführt? Ovoldsondichung, die eich auf eine mönnliche Offenbafund, gine Ausselbung oder andere Maßnahmen Dazie eine Berutzung, dies eine Ausselbung oder anderen Maßnahmen bezie eine Berutzung, dies Ausselbung oder anderen Maßnahmen bezie	The Space Mediterstrive rig. die nach dem internationalen Armeldedatum neier dem Prioritätsdatum verüfentlicht worden ist und mit der Armeldung nicht kolfidert, sondem nur zum Verstrinnste den den Erfindung nicht kolfidert, sondem nur zum Verstrinnste den den Erfindung zugundellegenden Priuzpa oder der ihr zugrundellegenden Theode engegoben ist "Veröffentlichtung von besonderer Bedeutung; die beamspruchte Erfindungst erfordentscher Tätigkeit beruhend betrachte der veröffentlichtung und deser Veröffentlichtung; die beamspruchte Erfindungt (wie veröffentlichtung und beschieber Bedeutung; die beamspruchte Erfindungt (wie veröffentlichtung und beschieber Tätigkeit beruhend betrachtet veröffentlichtung und deser Kategobe in Veröffentlichtungen dieser Kat
Veröffenfletung, de vor eine materialisten veröfenflicht werden ich dem besinspruchten Prioritätsdatum veröffenflicht werden ich Datum des Abschlüsses der Internativaktion Rochercho	Absendedatum des internationales Recherchenbestotts
17. Juli 2000	24/07/2000
The American State of the International on Recharcherbehinte	Bevolknächtigter Bediensteter
Name und Presentation Patricians, P.B. 5616 Patrician 3 NL = 2280 MV Rignets Tel. (+31-70) 340-3016 Fex. (+31-70) 340-3016	Leouffre, M

1

TOZON DI TOTALITATA E CONTRACTOR DE CONTRACT

INTERNATIONALER RECHERCHENBERICHT

Angaben 24 Verörfentschungen, die zur zeiden Pateintamike gehoren

Int. .orales Attengoichen
PCT/DE 00/00752

im Racharchanbaricht angeführtes Patentdokument	Datum der Veräffentlichung	Mitglied(er) der Patentlamilie	Datum der Veröffentlichung	_
DE 19718103 A	04-06-1998	AU 6354598 A CN 1207533 A EP 0875871 A JP 10341224 A US 6078908 A	05-11-1998 10-02-1999 04-11-1998 22-12-1998 20-06-2000	

Formulat PCT/85A2210 (Anhung Pownstrette) (LUE 1992)

INTERNATIONAL SEARCH REPORT

Ins. Monet Application No PCT/DE 00/00752

TPC 7	A CLASSIFICATION OF SUBJECT MATTER 1PC 7 H04Q7/38 G07F7/10 H04L29/06						
	international Patent Classification (IFC) or to both restoral classification	and IPC					
Minimum do	illo4Q CO7F HOAL	symbols) -					
Documentat	on searched other than minimum decembers to the extent that our	h documents are included in the fields so	RICHAN				
	•						
Electronia 4	ata base consulted during the international search (name of data base	and, where practical, search terms used)					
EPO-In							
Ĭ							
	ENTS CONSIDERED TO BE RELEVANT Citation of document, with makestion, where appropriate, of the release	/arn peasages	Relevant to claim No.				
Category *	CHRESON OF GOODWINE, WAS INTERESTED IN						
X	DE 197 18 103 A (SCHMITZ KIM)		1,4,6-9				
ļ	4 June 1998 (1998-06-04) the whole document	ļ					
1.	GSM TECHNICAL SPECIFICATION GSM	11.14	2,3				
A	VERSTON 5 7 0"						
	EUROPEAN TELECOMMUNICATION STANDARD, XX.XX. 1 April 1998 (1998-04 01), page						
	COMPLETE66 XP002089350						
1	page 12 -page 13						
		•					
1	}						
1							
Further donorments are listed in the continuation of box C. X Patent tamily members are tisted in the continuation of box C.							
* Special categories of cited documents: "T' later rivers make after the International Stind date or calculate and not in conflict with the application but							
'A' docum	"A" document defining the general state of the sit which is not crited to understand the principle or deality described to the sit which is not crited to understand the principle or deality described to the sit which is not crited to understand the principle or deality described to the sit which is not crited to understand the principle or deality described to the sit which is not crited to understand the principle or deality described to the sit which is not crited to understand the principle or deality described to the sit which is not crited to understand the principle or deality described to the sit which is not crited to understand the principle or deality described to the sit which is not crited to understand the principle or deality described to the sit which is not crited to understand the principle or deality described to the sit which is not crited to understand the principle or deality described to the sit which is not crited to understand the principle or deality described to the sit which is not crited to understand the principle or deality described to the sit which is not crited to understand the principle or deality described to the sit which is not crited to the sit which i						
E earlier dramment but published on or after the International **X* dramment of purely at the contraduct to cont							
which is cited to establish the publication date of another "Y" document of puriousisr relevances the claimed inventor an inventor and inventor of purious an inventor of purious and purious and inventor of purious and inventor of purious and inve							
"O" thusament is combined with one of more other such other means such combination being obvious to a person stilled							
SE docum	"E" document published prior to the internative of Eing date but "E" document member of the same puter family						
	Case of the secural completion of the international country						
	12 July 2000	24/07/2000					
Name an	d mailing address of the ISA European Paters Ottice, P.B. 5818 Petensaan 2	Authorized officer					
	5.xrupush Paters (2006, 173, 5010 Potential 2 NL - 2290 IV (Lipski) Tel. (+01-70) 340-2040, Tx. 81 651 epo m. Fax (+01-70) 340-3016	Leouffre, M					

Th Roll Demandaries

INTERNATIONAL SEARCH REPORT

information on fatout touck member

Int Bonsi Application No PCT/DE 00/00752

		.01,00		
Patent document cited in search report	Publication date	Patent family member(c)	Publication date	
DE 19718103 A	04-06-1998	AU 6354598 A CN 1207533 A EP 0875871 A JP 10341224 A US 6078908 A	05-11-1998 10-02-1999 04-11-1998 22-12-1998 20-06-2000	